



INTELLIGENCE COMMUNITY STANDARD

107-01

Continued Retention of SIGINT Under PPD-28

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; Presidential Policy Directive 28/PPD-28, Signals Intelligence Activities; Intelligence Community Directive (ICD) 107, Civil Liberties and Privacy, and other applicable provisions of law.

B. PURPOSE: This document establishes a process to seek a determination by the Director of National Intelligence (DNI) that continued retention of personal information of non-U.S. persons collected through Signals Intelligence (SIGINT) for which no permanent retention decision has been made under Section 4 of PPD-28 is in the national security interests of the United States.

1. PPD-28, Section 4(a)(i), provides that Intelligence Community (IC) elements may retain personal information concerning non-U.S. persons collected through SIGINT only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and that such information shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Personal information collected through SIGINT for which no permanent retention decision has been made under Section 4 of PPD-28 shall not be retained for more than five years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.

2. This Standard provides specific procedures for IC elements to seek the DNI's determination that continued retention of personal information of non-U.S. persons collected through SIGINT for which no permanent retention decision has been made under Section 4 of PPD 28 is appropriate beyond five years, and guidelines for how such requests will be evaluated. This document is not intended to alter the retention periods allowed by procedures approved by the Attorney General under EO 12333, Section 2.3, the rules applicable under the Foreign Intelligence Surveillance Act or orders issued pursuant to the Act, or to restrict or interfere with retention necessary to satisfy obligations imposed by law, such as discovery or preservation obligations imposed by a U.S. Federal court. For data that is covered by both PPD-28 and Section 309 of the Intelligence Authorization Act of 2015, IC elements must comply with both PPD-28 and Section 309.

C. APPLICABILITY: This document applies to the IC as defined by the National Security Act of 1947, as amended; and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the DNI and the head of the department or agency concerned.

D. IMPLEMENTATION

1. The head of an IC element that has collected personal information of non-U.S. persons through SIGINT, or his or her designee, may submit a request to the DNI seeking a determination that the continued retention of that information is in the national security interests of the United States. All requests for continued retention shall be submitted to the DNI by the IC element that originally collected the SIGINT. For joint collection activities, either party may submit the request to the DNI. Where the SIGINT has been shared with other IC elements, those elements shall submit their requests through the IC element that originally collected that information.

2. Depending on the nature of the information, requests for continued retention may be submitted for discrete datasets, data collected from particular collection sources, data pertaining to a particular event or intelligence topic, or similar types of information. Requests shall be as narrowly tailored as possible. At a minimum, each request shall include:

- a. A description of the information that has been identified for continued retention, including the nature and sensitivity of the personal information;
- b. A representation that the information has been lawfully collected in accordance with Part 1 of Executive Order 12333, and in a manner consistent with PPD-28 and all other legal authorities;
- c. A specific length of time for the extension (including whether the element is requesting that the extension be approved for subsequently acquired information) and an explanation of why that length of time is appropriate;
- d. The specific mission need(s) for continued retention of the information, including supporting documentation of the information's potential foreign intelligence or counterintelligence value (continued retention of information about the routine activities of foreign persons would not be justified without some indication that the information is otherwise valuable for an authorized intelligence purpose);
- e. A description of the safeguards that will be implemented to protect the information from improper access or use during the extended retention period, including any additional safeguards deemed necessary;
- f. The views on the adequacy of the proposed protections from the senior official responsible for matters involving the protection of civil liberties and privacy (designated or identified by the IC element head pursuant to Section E.2.b. of ICD 107);
- g. Whether the relevant information is available to or has been provided to other IC elements; and
- h. Any limitations on the initial retention of the information by the IC element that originally collected the SIGINT.

3. Except in exigent circumstances or because of changing mission requirements, requests for the continued retention of personal information of non-U.S. persons collected through SIGINT should be submitted at least 180 days before the end of the current period for which retention is authorized by applicable PPD-28 implementing procedures. Elements shall prioritize requests and submit them quarterly.

4. Personal information acquired by an IC element on or before the effective date of this Standard that has been identified as being obtained from SIGINT (Section E.1.a.), and for which no permanent retention decision has been made under Section 4 of PPD-28, may not be retained beyond five years from the effective date of this Standard unless the continued retention has been authorized by the DNI through the process established by this document. For personal information acquired after the effective date of this Standard, the five-year retention periods begin on the date of acquisition. The following types of SIGINT information are not subject to this five-year retention rule:

- a. Information that has not been processed into an intelligible form because of unknown communication methods, encryption, or other methods of concealing secret meaning (the five-year retention period for such information begins when the information has been made intelligible);
- b. Information necessary to avoid unauthorized collection, retention, or dissemination; or to avoid the collection, retention, and dissemination of information that is not foreign intelligence information;
- c. Information necessary to test or develop signals intelligence capabilities;
- d. Information retained for data integrity backup purposes, provided that only personnel responsible for maintaining those backups have access to such information. In the event that information retained for backup purposes must be restored, elements shall apply these procedures to the restored information. Information will be retained for data backup purposes for such time as reasonably necessary; and
- e. Information necessary to satisfy obligations imposed by law, such as discovery or preservation obligations imposed by a U.S. federal court, or for the performance of lawful oversight functions of personnel or systems, including lawful oversight functions of Congress, the Department of Justice, the Office of the Director of National Intelligence, the applicable Offices of the Inspectors General, or for other authorized oversight bodies.

5. In determining whether to approve a request for continued retention as being in the national security interests of the United States, the DNI will consider all the relevant circumstances, including: whether the requested extension is appropriate to carry out an authorized mission of the element(s) that will retain or access the information; the value of the foreign intelligence or counterintelligence that the information is reasonably likely to contain; the nature and sensitivity of the personal information being retained; the length of time for which the information will be retained; and the adequacy of existing or additional civil liberties and privacy protections that will be applied. The DNI will also consider the views provided for in Section D.2.f.

6. Requests may be approved in their entirety or in part (including making approval contingent on the implementation of additional safeguards), returned for further action, or disapproved. The DNI will take appropriate action within 90 days of receiving the complete submission. Requests will generally not be approved for a period to exceed five years.

E. ROLES AND RESPONSIBILITIES:

- 1. Heads of IC elements shall:

a. Take reasonable measures to identify the SIGINT collected by and held by that element for which no retention decision has been made by any IC element but which is subject to the requirements of PPD-28 and this Standard. The head of an IC element shall, by January 1, 2016, provide the DNI a description of the measures taken to identify SIGINT within their holdings as described in this section;

b. Submit any requests for extension of the initial retention period for all SIGINT originally collected by that IC element; and

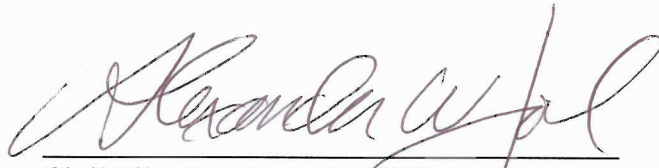
(1) Prioritize and submit such requests for the continued retention of information described in this Standard no later than 180 days before the end of the authorized retention period (Section D.4.); and

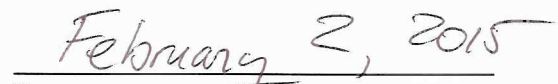
(2) Review requests for extension received from an IC element with which SIGINT has been shared and submit corresponding requests to the DNI as appropriate.

c. As the recipient of SIGINT shared by another IC Element, submit requests for extension of the initial retention period to the IC element that originally collected the SIGINT.

2. The Deputy Director for Intelligence Integration shall, in coordination with ODNI Civil Liberties Protection Officer, ODNI General Counsel, and the Assistant DNI for Policy and Strategy, prepare an assessment of each request by an IC element and provide a recommendation to the DNI, which will include any specific recommendations of each coordinating office.

F. EFFECTIVE DATE: This Standard becomes effective on the date of signature.


Civil Liberties Protection Officer


Date